PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-122539
(43)Date of publication of application : 28.04.2000

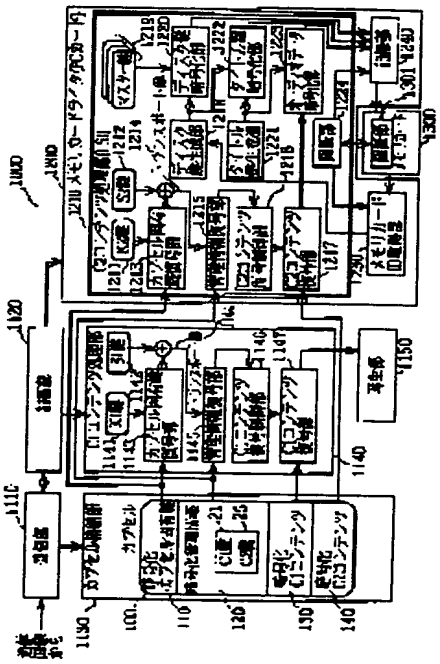
(51)Int.Cl. G09C 1/00
G06F 12/14
G11B 20/10
H04L 9/10

(21)Application number : 10-295837
(22)Date of filing : 16.10.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
HARADA TOSHIHARU

(54) BOOK PROTECTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a book protection system preventing deciphered contents from being illegally peeped into during a recording process after ciphered contents are deciphered once and re-ciphered.
SOLUTION: A personal computer receives a capsule 100 containing ciphered C2 contents 140 from a communication line, and the C2 contents are deciphered by a C2 contents deciphering part 1217 in a C2 contents processing part 1210 which is a tamper-resistant LSI package in a memory card writer 1200 of a PC card, and an audio data ciphering part 1223 ciphers the entire or a part of the deciphered C2 contents and outputs it to a recording part 1240. The recording par 1240 records the data ciphered in the C2 contents processing part 1210 on a memory card 1300 which is a semiconductor memory inserted into a memory card writer 1200.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－122539
（P2000－122539A）
(43)公開日　平成12年４月28日(2000.4.28)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｂ０１７
	６２０		６２０Ｚ	５Ｄ０４４
	６４０		６４０Ｂ	５Ｊ１０４
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	

審査請求　未請求　請求項の数14　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平10－295837

(22)出願日　平成10年10月16日(1998.10.16)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

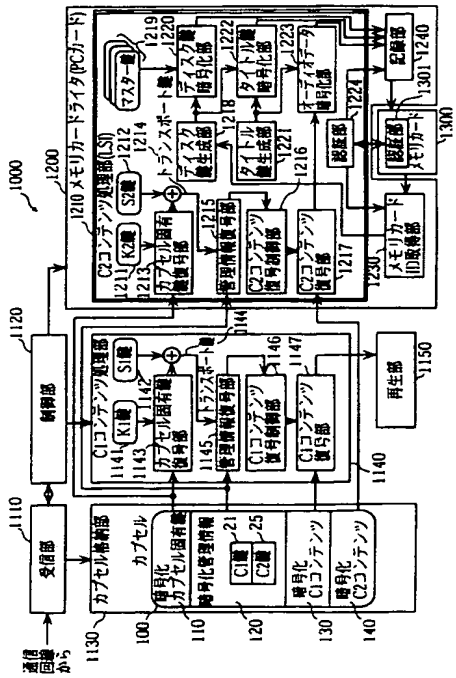
(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　著作物保護システム

(57)【要約】
【課題】　暗号化されたコンテンツを一度復号して再度暗号化して記録媒体に記録する過程において、復号されたコンテンツが不正に覗き見されないような著作物保護システムを提供する。
【解決手段】　パーソナルコンピュータにより、暗号化Ｃ２コンテンツ１４０を含むカプセル１００を通信回線から受信し、Ｃ２コンテンツを、ＰＣカードであるメモリカードライタ１２００中の耐タンパ性のあるＬＳＩパッケージであるＣ２コンテンツ処理部１２１０内でＣ２コンテンツ復号部１２１７により復号し、その復号したＣ２コンテンツの全部又は一部をオーディオデータ暗号化部１２２３が暗号化して記録部１２４０に出力する。記録部１２４０は、メモリカードライタ１２００に挿入された半導体メモリであるメモリカード１３００に、Ｃ２コンテンツ処理部１２１０内で暗号化されたデータを記録する。



1

【特許請求の範囲】

【請求項１】　外部から入力されたデジタル著作物である暗号化されたコンテンツを復号し、再暗号化して出力する著作物保護システムであって、

入力されたコンテンツを第１の暗号方式で復号する復号手段と、

前記復号手段により復号されたコンテンツの全部又は一部を第２の暗号方式で暗号化して出力する暗号化手段とを備え、

前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータの通信路が単一の耐タンパ性のあるパッケージに封入され、

外部との入出力のための端子が前記パッケージの外部に表出しており、

前記復号手段は、前記端子を通じて入力を受け付け、前記暗号化手段は、前記端子を通じて出力することを特徴とする著作物保護システム。

【請求項２】　前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータ通信路は、１チップの半導体集積回路から構成されていることを特徴とする請求項１記載の著作物保護システム。

【請求項３】　前記復号手段あるいは前記暗号化手段は、鍵データを記憶しており、復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムを、前記端子を通じて外部ネットワークよりダウンロードし、前記コンテンツを前記鍵データを用いて前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記鍵データを用いて前記暗号アルゴリズムにより暗号化することを特徴とする請求項１又は２記載の著作物保護システム。

【請求項４】　前記復号手段はさらに、前記端子を通じてコンテンツの復号に関する暗号化された制御情報を取得すると共に取得した制御情報を復号する制御情報復号部と、

前記復号部により復号された制御情報に基づいて前記コンテンツの復号を行うコンテンツ復号部とを有することを特徴とする請求項１～３記載のいずれか１項に記載の著作物保護システム。

【請求項５】　前記暗号化手段は、

マスター鍵を記憶するマスター鍵記憶部と、

ディスク鍵を生成するディスク鍵生成部と、

前記マスター鍵を用いて、前記ディスク鍵生成部により生成された前記ディスク鍵を暗号化するディスク鍵暗号化部と、

タイトル鍵を生成するタイトル鍵生成部と、

前記ディスク鍵を用いて、前記タイトル鍵生成部により生成された前記タイトル鍵を暗号化するタイトル鍵暗号化部と、

前記タイトル鍵を用いて、前記復号手段により復号されたコンテンツの一部又は全部のデータを暗号化するデータ暗号化部と、

2

前記ディスク鍵暗号化部により暗号化されたディスク鍵と、前記タイトル鍵暗号化部により暗号化されたタイトル鍵と、前記データ暗号化部により暗号化されたデータとを前記端子を通じて出力する出力部とを有することを特徴とする請求項１～４のいずれか１項に記載の著作物保護システム。

【請求項６】　前記マスター鍵記憶部は、複数のマスター鍵を記憶し、

前記ディスク鍵暗号化部は、複数の前記マスター鍵それぞれを用いて、前記ディスク鍵を暗号化することにより、複数の暗号化されたディスク鍵を生成することを特徴とする請求項５記載の著作物保護システム。

【請求項７】　前記暗号化手段はさらに、

前記マスター鍵を外部ネットワークよりダウンロードして前記マスター鍵記憶部に追加する、あるいは、特定マスター鍵を無効化するマスター鍵制御部を有することを特徴とする請求項５又は６記載の著作物保護システム。

【請求項８】　前記暗号化手段により暗号化の結果として得るデータは、記録媒体に記録されるべきものであり、

前記記録媒体には、予め媒体に固有な固有情報が記録されており、

前記ディスク鍵生成部は、前記記録媒体中の前記固有情報に基づいて前記ディスク鍵を生成することを特徴とする請求項５～７のいずれか１項に記載の著作物保護システム。

【請求項９】　前記タイトル鍵生成部は、前記復号手段により復号されたコンテンツの一部の情報、又は前記暗号化手段に固有な情報に基づき、前記タイトル鍵を生成することを特徴とする請求項５～８のいずれか１項に記載の著作物保護システム。

【請求項１０】　前記記録媒体は、記録装置認証部を備え、

前記出力部は、前記記録媒体の前記記録装置認証部から受信する認証情報に基づいて前記記録媒体の正当性を判定し、正当である場合にのみ、前記出力を行うことを特徴とする請求項５～９のいずれか１項に記載の著作物保護システム。

【請求項１１】　前記復号手段は、前記コンテンツの復号に際し、当該復号に対する課金処理を行うことを特徴とする請求項１～１０記載の著作物保護システム。

【請求項１２】　前記復号手段あるいは前記暗号化手段は、外部ネットワークよりダウンロードした復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムについて署名情報を確認して、正当であった場合にのみ、以後、前記コンテンツを前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記暗号アルゴリズムにより暗号化することを特徴とする請求項３記載の著作物保護システム。

【請求項１３】　前記マスター鍵制御部は、外部ネットワークよりダウンロードした前記マスター鍵について署名情報を確認して、正当であった場合にのみ、前記マスター鍵を前記マスター鍵記憶部に格納する、あるいは、無効化制御について、著名情報を確認して、正当であった場合にのみ、前記特定マスター鍵の無効化を行うことを特徴とする請求項７記載の著作物保護システム。

【請求項１４】　前記パッケージは、記録媒体に前記コンテンツを記録する記録装置に内蔵され、

前記暗号化手段は、前記記録媒体に前記コンテンツの全部又は一部を記録するための所定の規格化された暗号化方式に従った暗号化を行うものであり、

前記復号手段に入力される前記コンテンツに施されている暗号化は、前記コンテンツの配送元と、前記記録装置との間における特有の暗号化方式により、前記コンテンツを安全に配送するためになされたものであることを特徴とする請求項１又は２記載の著作物保護システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル著作物の著作権保護技術に関し、特に、ネットワークを介して配送されるコンテンツを記録媒体に記録する場合に用いる著作権保護技術に関する。

【０００２】

【従来の技術】近年、インターネット関連技術の発展により、音楽等のコンテンツをインターネットを通じて配送し、これをダウンロードしたユーザから料金等を受け取ることも可能となってきた。また、インターネットからパーソナルコンピュータにダウンロードされたディジタル著作物が簡単に複製できるものであるため、これを防止するために、暗号化技術を用いてコンテンツを暗号化して配送することも可能である。

【０００３】

【発明が解決しようとする課題】ネットワークを介して配送する有償のコンテンツが不正にコピー等されることを回避するために、コンテンツの提供者は、インターネット等を通じてコンテンツを暗号化して配送し、購入者は、配送されたコンテンツを専用の記録媒体に記録した後、その記録媒体を専用の再生装置に挿入して再生させることができるというようなコンテンツの流通形態が考えられる。この場合、コンテンツの内容は専用の記録媒体においても暗号化されるべきであるが、専用の記録媒体を小型化することその他の目的により専用の記録媒体においては、ネットワーク上で配送されるための暗号化とは異なる暗号化、例えばより小規模のアルゴリズムで実現できる暗号化を施す必要がある場合もある。また、記録媒体への記録のための暗号化について、各メーカ間の協議により規格化されている場合もある。なお、この場合、この規格に従って記録された記録媒体は、各メーカの再生装置で再生可能となる。

【０００４】しかしながら、ネットワーク上で配送されるために暗号化されたコンテンツを、一度復号してから再度記録媒体に記録するための暗号化を施すと、復号から再暗号化までの経路において、復号されたコンテンツが不正に覗き見される危険が生じる。そこで、本発明は、このような問題点に鑑みてなされたものであって、暗号化されたコンテンツを一度復号して再度暗号化して記録媒体に記録する過程において、復号されたコンテンツが不正に覗き見されないような著作物保護システムを提供することを目的とする。

【０００５】

【課題を解決するための手段】上記課題を解決するために、本発明に係る著作物保護システムは、例えばネットワークを介して、外部から入力されたデジタル著作物である暗号化されたコンテンツを復号し、記録用に再暗号化して出力する著作物保護システムであって、入力されたコンテンツを第１の暗号方式で復号する復号手段と、前記復号手段により復号されたコンテンツの全部又は一部を第２の暗号方式で暗号化して出力する暗号化手段とを備え、前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータの通信路が単一の耐タンパ性のあるパッケージに封入され、外部との入出力のための端子が前記パッケージの外部に表出しており、前記復号手段は、前記端子を通じて入力を受け付け、前記暗号化手段は、前記端子を通じて出力することを特徴とする。

【０００６】上記構成により、暗号化されたコンテンツを一度復号して再度暗号化する過程において、復号されたコンテンツが不正に覗き見されないようになる。

【０００７】

【発明の実施の形態】以下、本発明に係る著作物保護システムの実施の形態である音楽コンテンツ再生記録システムについて、図面を用いて説明する。

＜構成＞図１は、本発明の実施の形態に係る音楽コンテンツ再生記録システム１０００の外観図である。

【０００８】音楽コンテンツ再生記録システム１０００は、通信回線１００１を介して受信した音楽コンテンツをパーソナルコンピュータ１１００により再生し、また、メモリカード１３００に記録するシステムである。なお、メモリカード１３００は、厚さ数ミリ、縦横２ｃｍ四方程度の形状で、６４メガバイトの記憶容量をもち制御回路を内蔵する半導体メモリである。ユーザは、このメモリカード１３００を、メモリカード再生機器に挿入することにより、ヘッドフォン等を通じて再生された音楽を楽しむことができる。

【０００９】同図に示すように、音楽コンテンツ再生記録システム１０００は、ディスプレイ１１９１とキーボード１１９２とを備えるパーソナルコンピュータ１１００と、これに挿入されるメモリカードライタ１２００とから構成される。パーソナルコンピュータ１１００は、

ＣＰＵ、メモリ、ハードディスク等を内蔵し、ユーザに指示に応じて音楽コンテンツ再生用のプログラムを実行することができるものであり、スピーカ１１９３及び通信回線１００１と接続されており、また、いわゆるＰＣカードスロットであるメモリカードライタ挿入口１１９５を有する。

【００１０】メモリカードライタ１２００は、いわゆるＰＣカードであり、メモリカードを挿入するためのメモリカード挿入口１２９９を有している。図２は、音楽コンテンツ再生記録システム１０００の機能ブロック図である。機能的には、音楽コンテンツ再生記録システム１０００は、受信部１１１０と、制御部１１２０と、カプセル格納部１１３０と、Ｃ１コンテンツ処理部１１４０と、再生部１１５０と、メモリカードライタ１２００とから構成される。同図には、音楽コンテンツ再生記録システム１０００自体の他、メモリカードライタ１２００に挿入されるメモリカード１３００と、通信回線から受信部１１１０が受信してカプセル格納部１１３０に格納するカプセル１００とをも示している。ここで、カプセル１００は、通信回線から音楽コンテンツ再生記録システム１０００に入力されるデータであり、音楽コンテンツとこれに関する管理情報等が暗号化されたものである。カプセル１００の内容については後に詳しく説明する。

【００１１】受信部１１１０と、制御部１１２０と、Ｃ１コンテンツ処理部１１４０と、再生部１１５０とはパーソナルコンピュータ１１００のメモリに格納された音楽コンテンツ再生用のプログラムがＣＰＵにより実行されることによって実現される機能であり、カプセル格納部１１３０は、パーソナルコンピュータ１１００のメモリ又はハードディスクの一領域である。

【００１２】音楽コンテンツ再生用のプログラムは、受信すべき音楽コンテンツをユーザに選択させたり、選択された音楽コンテンツを再生するか、記録するか等のユーザの指示を受け付けるためのものであり、制御部１１２０は、キーボード１１９２によるユーザ操作を受け付け、これに応じて、音楽コンテンツの受信指示、再生指示、記録指示等を行うものである。

【００１３】受信部１１１０は、制御部１１２０からの受信指示を受けて、インターネットに接続された通信回線１００１から暗号化された音楽コンテンツを含むデータであるカプセルを受信して、カプセル格納部１１３０に格納し、カプセルの格納場所を制御部１１２０に通知する。カプセルは音楽コンテンツの供給会社等からインターネット等を通じて配送される。ここでは説明のため、図２に示すように、受信部１１１０によりカプセル格納部１１３０にはカプセル１００が格納されたものとする。

【００１４】Ｃ１コンテンツ処理部１１４０は、制御部１１２０から、再生指示とカプセル１００の格納場所についての情報とを受けると、カプセル１００中の暗号化Ｃ１コンテンツ１３０を復号するための処理を行い、復号したＣ１コンテンツを再生部１１５０に出力する。音楽コンテンツには、１６ＫＨｚのサンプリングレートでサンプリングされた低音質の試聴用のものと、６４ＫＨｚのサンプリングレートでサンプリングされた高音質の購入用のものとの２種類のものが存在し、ここでは、前者をＣ１コンテンツといい、後者をＣ２コンテンツという。暗号化Ｃ１コンテンツ１３０は、Ｃ１コンテンツを暗号化したものであり、暗号化Ｃ２コンテンツ１４０は、Ｃ２コンテンツを暗号化したものである。なお、Ｃ１コンテンツ処理部１１４０の詳細については、カプセル１００の内容と共に後に詳細に説明する。

【００１５】再生部１１５０は、Ｃ１コンテンツ処理部１１４０から渡されたＣ１コンテンツを再生してスピーカ１１９３を鳴らす機能部分であり、音楽コンテンツはＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）オーディオの規格に則って圧縮されているものであるため、再生部１１５０はこれを伸張する機能をも有する。

【００１６】メモリカードライタ１２００は、図３に示すようなハードウェア構造を有するＰＣカードであり、制御部１１２０から記録指示とカプセル１００の格納場所についての情報とを受け取ると、カプセル１００中の暗号化Ｃ２コンテンツ１４０を復号して再度別の暗号化を施してメモリカード１３００に記録する機能を有するものである。

【００１７】図３は、メモリカードライタ１２００のハードウェア構造を示す図である。同図に示すように、メモリカードライタ１２００は、ハードウェア的には、ＣＰＵ１２０１と、ＲＯＭ１２０２と、ＲＡＭ１２０３と、ＰＣインタフェース１２０４と、メモリカードインタフェース１２０５と、複数の端子をもつＬＳＩであるＣ２コンテンツ処理部１２１０とがバス接続されたものであり、ＰＣインタフェース１２０４を介してＰＣＭＣＩＡ（Ｐｅｒｓｏｎａｌ　ＣｏｍｐｕｔｅｒＭｅｍｏｒｙ　Ｃａｒｄ　Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ａｓｓｏｃｉａｔｉｏｎ）規格に従いパーソナルコンピュータ１１００とデータの通信を行い、メモリカードインタフェース１２０５を介してメモリカード１３００とデータの通信を行う。

【００１８】ここで、ＣＰＵ１２０１は、ＲＯＭ１２０２に記録されたプログラムを実行しメモリカードライタ１２００の制御を行うものであり、ＲＡＭ１２０３を作業用の領域として用いる。また、Ｃ２コンテンツ処理部１２１０は、電流供給用の導線で巻き付けられ全面的に包まれた耐タンパ性を有するＬＳＩパッケージである。耐タンパとは、外部からの不正なアクセスに対して防御可能なことである。Ｃ２コンテンツ処理部１２１０は、１つのシリコン基盤上に形成された、即ち、１チップの

集積回路である。また、Ｃ２コンテンツ処理部１２１０は、電気的、物理的に内部データを検査することが不可能となっており、例えば、ＬＳＩパッケージの内部データがＥＥＰＲＯＭに保持されており、ＬＳＩパッケージを開けようとすると導線が切断されることになり、これによりＬＳＩパッケージへの電流の供給が停止し、コンデンサに貯えられた電荷からなる内部データがクリアされるような構造となっている。

【００１９】メモリカードライタ１２００は、機能的には、図２に示すように、Ｃ２コンテンツを復号し、オーディオデータ記録用のための暗号化を施すＣ２コンテンツ処理部１２１０と、メモリカード１３００から個々のメモリカードに固有なメモリカードＩＤを取得するメモリカードＩＤ取得部１２３０と、暗号化されたオーディオデータをメモリカード１３００に記録する記録部１２４０とを備える。なお、Ｃ２コンテンツ処理部１２１０は、メモリカード１３００の正当性を認証するための認証部１２２４をも含む。Ｃ２コンテンツ処理部１２１０の処理内容の詳細については後述する。

＜データ構造と関連処理＞以下、カプセル１００の内容について説明する。カプセル１００は、著作権保護センタにより生成されるデータである。ここで著作権保護センタとは、著作権保護のための中立的な機関をいう。著作権保護センタは、上述した音楽コンテンツの供給会社等から音楽コンテンツとこれに関連する管理情報等を受け取り、これらを暗号化してカプセル１００を生成する。

【００２０】音楽コンテンツ再生記録システム１０００に入力されるカプセル１００は、図１に示すように、１６０ビットの暗号化カプセル固有鍵１１０と、固定長の暗号化管理情報１２０と、内容に応じてデータ長が変わり得る暗号化Ｃ１コンテンツ１３０と、内容に応じてデータ長が変わり得る暗号化Ｃ２コンテンツ１４０とから構成されるデータである。

【００２１】図４は、暗号化Ｃ１コンテンツ１３０及び暗号化Ｃ２コンテンツ１４０の生成過程を示すデータフロー図である。同図に示すように、暗号化Ｃ１コンテンツ１３０は、平文であるＣ１コンテンツ３０をＣ１鍵２１で暗号化することにより生成されるデータである。Ｃ１鍵２１は６４ビットの鍵データであり、暗号化はブロック暗号方式で行い、例えばＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）アルゴリズムが用いられる。

【００２２】また、暗号化Ｃ２コンテンツ１４０は、平文であるＣ２コンテンツ４０をＣ２鍵２５で暗号化することにより生成されるデータである。Ｃ２鍵２５は１２８ビットの鍵データであり、暗号化は、ブロック暗号方式で行い、例えばＤＥＳアルゴリズムに準じたアルゴリズムが用いられる。なお、Ｃ１コンテンツ３０及びＣ２コンテンツ４０はそれぞれ、ＭＰＥＧオーディオの規格に基づき圧縮されている。

【００２３】図５は、暗号化カプセル固有鍵１１０及び暗号化管理情報１２０の生成過程を示すデータフロー図である。同図に示すように、暗号化管理情報１２０は、管理情報２０をトランスポート鍵１１４４で暗号化することにより生成されるデータである。ここで、管理情報２０は、図４に示したＣ１コンテンツ３０及びＣ２コンテンツ４０に関連した情報であり、Ｃ１鍵２１、Ｃ１アドレス２２、Ｃ１復号条件情報２３、Ｃ１課金情報２４、Ｃ２鍵２５、Ｃ２アドレス２６、Ｃ２復号条件情報２７、Ｃ２課金情報２８を含む。また、暗号化３における暗号化アルゴリズムはブロック暗号方式のものであり、例えばＤＥＳアルゴリズムに準じたアルゴリズムが用いられる。

【００２４】ここで、Ｃ１アドレス２２及びＣ２アドレス２６は、それぞれカプセル１００内における暗号化Ｃ１コンテンツ１３０の相対アドレス、暗号化Ｃ２コンテンツ１４０の相対アドレスを示す。Ｃ１復号条件情報２３及びＣ２復号条件情報２７は、それぞれＣ１コンテンツ３０、Ｃ２コンテンツ４０を復号するための条件を示す情報であり、復号することを許容する期日等を示すものである。また、Ｃ１課金情報２４及びＣ２課金情報２８は、それぞれＣ１コンテンツ３０、Ｃ２コンテンツ４０を復号する際に請求されるべき料金に関する情報、即ち、音楽コンテンツの試聴料金や購入料金を示す情報である。

【００２５】トランスポート鍵１１４４は、著作権保護センタが任意に定める１６０ビットの鍵データである。また、図５に示すように、暗号化カプセル固有鍵１１０は、トランスポート鍵１１４４とＳ１鍵１１４２との排他的論理和により得られるカプセル固有鍵１０を、楕円秘密鍵５で、楕円暗号方式のアルゴリズムにより暗号化して生成されるデータである。ここで、Ｓ１鍵１１４２は、音楽コンテンツ再生記録システム１０００のＣ１コンテンツ処理部１１４０に記憶されているＳ１鍵と同値の１６０ビットの共通鍵である。また、楕円秘密鍵５は、Ｃ１コンテンツ処理部１１４０に記憶されている公開鍵であるＫ１鍵１１４１と対となる１６０ビットの秘密鍵である。なお、楕円暗号については、Ｄｏｕｇｌａｓ　Ｒ．Ｓｔｉｎｓｏｎ著「暗号理論の基礎」（共立出版株式会社）に詳細に説明されている。

【００２６】以下、上述のように生成されたカプセル１００の内容に関連した処理を行うＣ１コンテンツ処理部１１４０及びＣ２コンテンツ処理部１２１０の処理内容について詳細に説明する。まず、Ｃ１コンテンツ処理部１１４０の処理内容について説明する。Ｃ１コンテンツ処理部１１４０は、Ｋ１鍵１１４１及びＳ１鍵１１４２を記憶しており、また、カプセル固有鍵復号部１１４３と、管理情報復号部１１４５と、Ｃ１コンテンツ復号制御部１１４６と、Ｃ１コンテンツ復号部１１４７とを構

成要素とする。

【００２７】カプセル固有鍵復号部１１４３は、カプセル１００内の暗号化カプセル固有鍵１１０を、公開鍵であるＫ１鍵１１４１を用いて復号化して出力する。出力されたカプセル固有鍵と、共通鍵であるＳ１鍵１１４２との排他的論理和の結果であるトランスポート鍵１１４４を用いて、管理情報復号部１１４５は、カプセル１００内の暗号化管理情報１２０を復号する。

【００２８】Ｃ１コンテンツ復号制御部１１４６は、復号された管理情報２０中のＣ１復号条件情報２３を参照することにより復号可否を判断して、復号可能な場合には、Ｃ１課金情報２４を参照して課金処理を行い、Ｃ１コンテンツ復号部１１４７に復号指示を与える。ここで、課金処理とは、通信回線を介して、ユーザが予め契約している銀行等の口座から、音楽コンテンツの供給会社等に、試聴料金を送金するような旨の指示情報を送信することである。なお、試聴は無料である場合には、前記指示情報の送信は行わない。

【００２９】Ｃ１コンテンツ復号部１１４７は、管理情報復号部１１４５により復号された管理情報２０中のＣ１アドレス２２を参照して暗号化Ｃ１コンテンツ１３０の位置を特定し、管理情報２０中のＣ１鍵２１を用いて、暗号化Ｃ１コンテンツ１３０を復号し、再生部１１５０にＣ１コンテンツ３０を出力する。なお、復号アルゴリズムは、図４に示す暗号化１に対応するブロック暗号方式のアルゴリズムである。

【００３０】次に、Ｃ２コンテンツ処理部１２１０の処理内容について説明する。Ｃ２コンテンツ処理部１２１０の処理内容は、Ｃ２コンテンツの復号と、メモリカードへの記録のための再暗号化とに大別されるが、Ｃ２コンテンツの復号に関しては、上述のＣ１コンテンツ処理部１１４０の処理と類似している。Ｃ２コンテンツ処理部１２１０は、Ｃ２コンテンツの復号機能を行うために、Ｋ２鍵１２１１及びＳ２鍵１２１２を記憶し、カプセル固有鍵復号部１２１３と、管理情報復号部１２１５と、Ｃ２コンテンツ復号制御部１２１６と、Ｃ２コンテンツ復号部１２１７とを構成要素としており、さらに、メモリカードへの記録のための再暗号化機能を行うために、複数のマスター鍵１２１９を記憶し、ディスク鍵生成部１２１８と、ディスク鍵暗号化部１２２０と、タイトル鍵生成部１２２１と、タイトル鍵暗号化部１２２２と、オーディオデータ暗号化部１２２３と、認証部１２２４とを構成要素としている。ここで、マスター鍵とは、各メーカのメモリカード再生装置に保持されている鍵データと同値の鍵データであり、その内容は、各メーカ毎に異なる。記録すべきメモリカードが複数のメーカのメモリカード再生装置で再生できるように、Ｃ２コンテンツ処理部１２１０には、複数のメーカについてのマスター鍵１２１９が記憶されている。

【００３１】カプセル固有鍵復号部１２１３は、カプセル１００内の暗号化カプセル固有鍵１１０を、公開鍵であるＫ２鍵１２１１を用いて復号化して出力する。出力されたカプセル固有鍵と、Ｓ２鍵１２１２との排他的論理和の結果であるトランスポート鍵１２１４を用いて、管理情報復号部１２１５は、カプセル１００内の暗号化管理情報１２０を復号する。ここで、トランスポート鍵１２１４は、上述したＣ１コンテンツ処理部１１４０において得られたトランスポート鍵１１４４と同値である。なお、Ｋ２鍵１２１１とＳ２鍵１２１２とは、図５における楕円秘密鍵５を、公開鍵であるＫ２鍵１２１１に対応する楕円秘密鍵に置き換えるとともに、図５におけるＳ１鍵１１４２をＳ２鍵に置き換えても、図５に示すようにトランスポート鍵１１４４に基づいて暗号化カプセル固有鍵１１０が生成できるような関係にある鍵データである。

【００３２】Ｃ２コンテンツ復号制御部１２１６は、管理情報復号部１２１５により復号された管理情報２０中のＣ２復号条件情報２７を参照することにより復号可否を判断して、復号可能な場合には、Ｃ２課金情報２８を参照して課金処理を行い、Ｃ２コンテンツ復号部１２１７に復号指示を与える。Ｃ２コンテンツ復号制御部１２１６によりなされる課金処理は、Ｃ１コンテンツ復号制御部１２１６によりなされる課金処理と同様であり、通信回線を介して、ユーザが予め契約している銀行等の口座から、音楽コンテンツの供給会社等に、購入料金を送金するような旨の指示情報を送信することである。前記指示情報は、メモリカードライタ１２００のＰＣインタフェース１２０４を介してパーソナルコンピュータ１１００の制御部１１２０により通信回線１００１に転送される。なお、Ｃ２コンテンツ復号制御部１２１６は、カウンタ値を記憶し、Ｃ２コンテンツの復号毎にカウンタ値を１増加して、このカウンタ値と購入料金の積を求めることにより、例えば１日における購入料金合計の送金指示を夜間に通信回線を通じて行うこともできるものである。

【００３３】Ｃ２コンテンツ復号部１２１７は、管理情報復号部１２１５により復号された管理情報２０中のＣ２アドレス２６を参照して暗号化Ｃ２コンテンツ１４０の位置を特定し、管理情報２０中のＣ２鍵２５を用いて、暗号化Ｃ２コンテンツ１４０を復号し、オーディオデータであるＣ２コンテンツをオーディオデータ暗号化部１２２３に伝える。なお、復号アルゴリズムは、図４に示す暗号化２に対応するブロック暗号方式のアルゴリズムである。

【００３４】また、認証部１２２４は、メモリカード１３００に含まれる認証部１３０１との間で、相互に認証をする機能を司る。認証部１３０１は、メモリカードへデータの記録を行う装置側の正当性を認証するもので、認証部１２２４は認証部１３０１から認証情報を受信して、この認証情報に基づいて前記メモリカードの正当性

を判断するものである。なお、認証の方法としては、例えば、メモリカードライタ１２００の認証部１２２４が乱数をメモリカード１３００の認証部１３０１に送り、認証部１３０１がこの乱数を秘密の暗号化アルゴリズムにより暗号化して返却するのを受けて、暗号化された乱数を認証部１２２４が復号アルゴリズムにより復号した結果が、もとの乱数と同値であれば、認証部１３０１が有する暗号化アルゴリズムと、認証部１２２４が有する復号アルゴリズムが対応するものであるので、認証に成功したと判断する方法が用いられる。この認証方法は、メモリカードライタ１２００と、メモリカード１３００とが、秘密の認証鍵と認証方法を共有し、前記認証鍵を用いたチャレンジレスポンス手順により相互に相手を認証する方法でもよい。

【００３５】認証が成功した場合、即ち、メモリカードが正当であると判断した場合には、認証部１２２４は、メモリカードライタ１２００のメモリカードＩＤ取得部１２３０及び記録部１２４０に、それぞれＩＤ取得許可、記録許可の指示を与える。ＩＤ取得許可を受けると、メモリカードＩＤ取得部１２３０は、メモリカード１３００から固有情報であるメモリカードＩＤを取得し、これをディスク鍵生成部１２１８に与え、また、記録許可を受けると、記録部１２４０は、ディスク鍵暗号化部１２２０、タイトル鍵暗号化部１２２２及びオーディオデータ暗号化部１２２３から出力される暗号化されたデータをメモリカード１３００に記録する。

【００３６】ディスク鍵生成部１２１８は、メモリカードＩＤ取得部１２３０から与えられたメモリカードＩＤに関する情報を一部に含むような６４ビットのディスク鍵を生成する。ここで、ディスク鍵とは、記録媒体であるメモリカード全体にわたって共通な鍵データを意味する。ディスク鍵暗号化部１２２０は、ディスク鍵生成部１２１８により生成されたディスク鍵を、予め記憶している複数のマスター鍵のうちの１つを用いて暗号化し、同じディスク鍵を、続けて別のマスター鍵を用いて暗号化する処理を繰り返し、マスター鍵の数と同じ数の暗号化ディスク鍵を生成してメモリカードライタ１２００内の記録部１２４０に出力する。

【００３７】タイトル鍵生成部１２２１は、適当な６４ビットのタイトル鍵を生成してタイトル鍵暗号化部に与える。ここで、タイトル鍵とは、音楽コンテンツ毎に設定できる鍵データを意味する。タイトル鍵暗号化部１２２２は、タイトル鍵生成部１２２１により生成されたタイトル鍵を、ディスク鍵生成部１２１８により生成されたディスク鍵を用いて暗号化して記録部１２４０に出力する。また、オーディオデータ暗号化部１２２３は、Ｃ２コンテンツ復号部１２１７により出力されたＣ２コンテンツを、タイトル鍵生成部１２２１により生成されたタイトル鍵で暗号化して、記録部１２４０に出力する。

【００３８】ディスク鍵暗号化部１２２０、タイトル鍵暗号化部１２２２及びオーディオデータ暗号化部１２２３による暗号化アルゴリズムは、ブロック暗号方式のＤＥＳアルゴリズムである。なお、記録部１２４０は、メモリカード１３００中のユーザアクセス可能領域にオーディオデータ暗号化部１２２３から受け取ったオーディオデータを記録し、メモリカード１３００中のユーザアクセスが不可能なシステム領域に暗号化されたディスク鍵及びタイトル鍵を記録する。また、メモリカード１３００を挿入可能なメモリカード再生機器は、マスター鍵を保持しているものであり、メモリカード１３００の認証に成功すれば、暗号化されたディスク鍵とタイトル鍵とを用いて、上述した記録のための暗号化処理の逆処理を行いオーディオデータを復号することにより音楽を再生する機能を有する。＜動作＞以下、上述の構成を備える音楽コンテンツ再生記録システム１０００の動作について説明する。

【００３９】図６は、音楽コンテンツ再生記録システム１０００の動作を示すフローチャートである。同図に示すように、まず、音楽コンテンツ再生記録システム１０００の受信部１１１０は、ユーザ指示に応じて、音楽コンテンツ供給会社のサーバからインターネットを通じて音楽コンテンツを含むカプセルを受信し、カプセル格納部１１３０に格納する（ステップＳ３０１）。

【００４０】これにより、カプセル格納部１１３０にカプセル１００が格納された場合、制御部１１２０は、音楽コンテンツの試聴、購入、又は処理終了のいずれかをユーザに選択させるための、グラフィカルユーザインタフェース画面をディスプレイ１１９１に表示する。この後、制御部１１２０は、ユーザが試聴を選択したことを検出すると（ステップＳ３０２）、Ｃ１コンテンツ処理部１１４０に、Ｃ１コンテンツの再生指示を行う。これを受けてＣ１コンテンツ処理部１１４０は、カプセル固有鍵復号部１１４３によりカプセル固有鍵を復号し、管理情報復号部１１４５により管理情報を復号する（ステップＳ３０３）。

【００４１】管理情報復号部１１４５により管理情報が復号された後、Ｃ１コンテンツ復号制御部１１４６は、Ｃ１復号条件情報２３を参照して、例えば、現在、Ｃ１コンテンツの試聴許容期限内の日時であることや復号回数が所定回数以内であること等によりＣ１復号条件が満たされている場合には（ステップＳ３０４）、課金処理を行い（ステップＳ３０５）、Ｃ１コンテンツ復号部１１４７によりＣ１コンテンツの復号を行い（ステップＳ３０６）、再生部１１５０により、Ｃ１コンテンツを再生してスピーカ１１９３を鳴らせる（ステップＳ３０７）。また、Ｃ１コンテンツの試聴許容期限の経過後のようにＣ１復号条件が満たされていない場合には（ステップＳ３０４）、ステップＳ３０５からステップＳ３０７の処理は行わない。

【００４２】また、制御部１１２０は、ユーザが購入を

選択したこと、即ちユーザがメモリカードへの記録を要求していることを検出すると（ステップＳ３０８）、メモリカードライタ１２００のＣ２コンテンツ処理部１２１０に、Ｃ２コンテンツの再生指示を行う。これを受けてＣ２コンテンツ処理部１２１０は、カプセル固有鍵復号部１２１３によりカプセル固有鍵を復号し、管理情報復号部１２１５により管理情報を復号する（ステップＳ３０９）。　管理情報復号部１２１５により管理情報が復号された後、Ｃ２コンテンツ復号制御部１２１６は、Ｃ２復号条件情報２７を参照して、例えば、現在、Ｃ２コンテンツの購入許容期限内の日時である等によりＣ２復号条件が満たされている場合には（ステップＳ３１０）、課金処理を行い（ステップＳ３１１）、Ｃ２コンテンツ復号部１２１７によりＣ２コンテンツの復号を行った後（ステップＳ３１２）、メモリカードへの記録のための暗号化と記録の処理を行う（ステップＳ３１３）。また、Ｃ２コンテンツの購入許容期限の経過後のようにＣ２復号条件が満たされていない場合には（ステップＳ３１０）、ステップＳ３１１からステップＳ３１３の処理は行わない。

【００４３】また、制御部１１２０は、ユーザが処理終了を選択したことを検出すると（ステップＳ３１４）、試聴又は購入に関する処理はすべて終了するが、処理終了を選択しなければ、ステップＳ３０２に戻る。従って、ユーザは、試聴又は購入を何度も選択することができる。図７は、メモリカードへのオーディオデータの記録のための暗号化と記録処理を示すフローチャートである。

【００４４】同図に示すように、認証部１２２４は、メモリカード１３００を認証し（ステップＳ４０１）、認証に成功しなければ、暗号化及び記録は行わず、認証に成功した場合には（ステップＳ４０２）、以下の処理を行う。まず、メモリカードＩＤ取得部１２３０は、メモリカード１３００からメモリカードＩＤを取得しディスク鍵生成部１２１８に与える（ステップＳ４０３）。ディスク鍵生成部１２１８は、与えられたメモリカードＩＤに基づいてディスク鍵を生成する（ステップＳ４０４）。

【００４５】ディスク鍵暗号化部１２２０は、生成されたディスク鍵を複数のマスター鍵１２１９それぞれを用いて暗号化し（ステップＳ４０５）、暗号化した複数のディスク鍵を記録部１２４０を介してメモリカード１３００に記録する（ステップＳ４０６）。ディスク鍵の記録後、タイトル鍵生成部１２２１は、タイトル鍵を生成し、これをディスク鍵を用いて暗号化し（ステップＳ４０７）、暗号化されたタイトル鍵を記録部１２４０を介してメモリカード１３００に記録する（ステップＳ４０８）。続いて、オーディオデータ暗号化部１２２３は、Ｃ２コンテンツ復号部１２１７により復号されたＣ２コンテンツをタイトル鍵を用いて暗号化し、記録部１２４０を介してメモリカード１３００に記録する（ステップＳ４０９）。

【００４６】このように、音楽コンテンツ再生記録システム１０００は、ユーザの要求に応じて、音楽コンテンツの再生及びメモリカードへの記録を行うことができる。以上、本発明に係る著作物保護システムについて、実施の形態である音楽コンテンツ再生記録システムに基づいて説明したが、本発明はこれらの実施の形態に限られないことは勿論である。即ち、

（１）本実施の形態では、メモリカードにオーディオデータを記録するメモリカードライタは、ＰＣカードであることとしたが、これに限定されることはなく、パーソナルコンピュータと接続可能な機器であればよく、例えばＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）等により接続される機器であればよい。また、本実施の形態における受信部１１１０、制御部１１２０、カプセル格納部１１３０、Ｃ１コンテンツ処理部１１４０、再生部１１５０は、パーソナルコンピュータ１１００により実現されるものとしたが、パーソナルコンピュータ１１００は、メモリ及びＣＰＵを備えプログラム実行制御機能を有する家電機器であればよく、例えば、インターネット接続機能をもつテレビ受信機であってもよい。

【００４７】また、本実施の形態では、Ｃ２コンテンツ処理部１２１０は、電流供給用の導線で巻き付けられ全面的に包まれた耐タンパ性を有するＬＳＩパッケージであることとしたが、耐タンパ性を有すれば、導線で巻き付けられているような形態のものに限定されることはない。

（２）本実施の形態では、メモリカードライタ１２００内のＣ２コンテンツ復号部１２１７が復号したＣ２コンテンツであるオーディオデータを、メモリカードへ記録するために暗号化することとしたが、この他、直接的に再生することとしてもよい。この場合、メモリカードライタ１２００にスピーカを接続すると、そのスピーカから音楽が流れるようにもできる。

（３）本実施の形態では、１つのカプセルに１つの暗号化Ｃ１コンテンツと１つの暗号化Ｃ２コンテンツが含まれていることとしたが、１つのカプセルに暗号化Ｃ１コンテンツ又は暗号化Ｃ２コンテンツのいずれかのみが含まれていてもよく、また、複数の暗号化Ｃ１コンテンツや複数の暗号化Ｃ２コンテンツが含まれていてもよく、これらの含まれ方がカプセル毎に異なることとしてもよい。なお、カプセルにＣ１コンテンツが含まれる場合にのみ管理情報中にはＣ１コンテンツに関連する課金等の情報が含まれ、カプセルにＣ２コンテンツが含まれる場合にのみ管理情報中にはＣ２コンテンツに関連する課金等の情報が含まれるようにすればよい。

（４）本実施の形態では、Ｃ１鍵が６４ビット、Ｃ２鍵が１２８ビット等と、鍵データについての長さを示した

が、この長さに限定されることはない。Ｋ１鍵、Ｋ２鍵、Ｓ１鍵、Ｓ２鍵、トランスポート鍵もそれぞれ別個の長さであってもよい。なお、暗号化カプセル固有鍵１１０は、Ｋ１鍵で復号できる鍵とＫ２鍵で復号できる鍵とを合成したものとしていてもよく、また、トランスポート鍵の算出のための排他的論理和計算も、全ビットではなく、所定のビットの排他的論理和としてもよい。また、本実施の形態において示した暗号化アルゴリズムも、ＤＥＳアルゴリズム等に限定されることはない。また、Ｃ１コンテンツ復号部における復号アルゴリズム及びＣ２コンテンツ復号部における復号アルゴリズムは、通信回線を介してダウンロードすることができるように構成していてもよい。また、復号アルゴリズムをダウンロードする際には、署名情報を確認してそれが正当なものである場合にしか復号アルゴリズムを取り込まないこととしてもよい。なお、この場合、Ｃ２コンテンツについての復号アルゴリズムは、メモリカードライタ１２００中のＲＯＭ１２０２に含まれる転送用のプログラムをＣＰＵ１２０１が実行することとにより、パーソナルコンピュータ１１００からＰＣインタフェース１２０４を介してＣ２コンテンツ処理部１２１０に書き込まれることになる。また、ディスク鍵暗号化部１２２０、タイトル鍵暗号化部１２２２、及びオーディオデータ暗号化部１２２３における暗号アルゴリズムについても、上述の復号アルゴリズムと同様な方法で、ダウンロードや、署名確認等を行える構成としてもよい。

【００４８】ここで、署名情報の確認は、例えば、著作権保護のための中立的な機関により、復号アルゴリズムと署名情報とが送信されるとすると、署名情報は、秘密鍵により暗号化されているものであるため、ＲＯＭ１２０２にその秘密鍵に対応する公開鍵を予め記憶しておき、上述の転送用のプログラムの実行によって、その公開鍵を用いて署名情報を復号することにより確認を行うこととすればよい。

【００４９】また、本実施の形態ではＣ１鍵及びＣ２鍵は、管理情報中に含まれることとしたが、これに限定されることはなく、Ｃ１鍵はＣ１コンテンツ復号部に予め記憶されている鍵データであることとしてもよく、Ｃ２鍵はＣ２コンテンツ復号部に予め記憶されている鍵データであることとしてもよい。

（５）本実施の形態では、カプセルは通信回線を通じて送られるものとしたが、これに限定されることはなく、光ディスク等の記録媒体に格納されるものであってもよい。この場合、受信部１１１０が、カプセルを記録媒体から読み出してカプセル格納部１１３０に格納するようなものであればよい。

（６）本実施の形態では、タイトル鍵生成部１２２１は、適当にタイトル鍵を生成することとしたが、これに限定されることはなく、タイトル鍵生成部１２２１は、例えば、Ｃ２コンテンツ復号部１２１７の出力するＣ２コンテンツを参照して、曲名等のデータに基づいてタイトル鍵を生成するものであってもよく、また、管理情報復号部１２１５により復号された管理情報中のＣ２鍵を参照し、これに基づいてタイトル鍵を生成するものであってもよい。また、さらに、タイトル鍵生成部１２２１は、メモリカードライタ１２００に固有な値に基づいてタイトル鍵を生成するものであってもよい。

（７）本実施の形態では、ディスク鍵生成部１２１８は、メモリカードＩＤに基づいてディスク鍵を生成することとしたが、メモリカードＩＤと無関係にディスク鍵を生成するものとしてもよい。また、メモリカード中にマスター鍵により暗号化された媒体に固有な固有ディスク鍵が記録されているものとしてもよく、これに対応して、ディスク鍵生成部１２１８は、この固有ディスク鍵を、マスター鍵を用いて復号することにより、ディスク鍵を生成することとしてもよく、この場合には、ディスク鍵暗号化部１２２０は不要となり、従って記録部１２４０により暗号化したタイトル鍵及び暗号化したオーディオデータのみがメモリカードに書き込まれるようにすればよい。

（８）本実施の形態では、オーディオデータ暗号化部１２２３は、Ｃ２コンテンツであるオーディオデータを暗号化するものとしたが、Ｃ２コンテンツの一部を暗号化して出力することとしてもよい。

（９）本実施の形態では、マスター鍵はＣ２コンテンツ処理部内に予め複数記憶されていることとしたが、これに限定されることはなく、単数であってもよい。また、Ｃ２コンテンツ処理部は、通信回線及びパーソナルコンピュータを介して外部ネットワークからマスター鍵をダウンロードして取り込み記憶することとしてもよく、特定のマスター鍵を削除する機能を有するものであってもよい。また、マスター鍵をダウンロードする際には、署名情報を確認してそれが正当である場合にのみマスター鍵を取り込むこととしてもよい。なお、この場合、マスター鍵は、メモリカードライタ１２００中のＲＯＭ１２０２に含まれる転送用のプログラムをＣＰＵ１２０１が実行することとにより、パーソナルコンピュータ１１００からＰＣインタフェース１２０４を介してＣ２コンテンツ処理部１２１０に書き込まれることになる。ここで、マスター鍵についての署名情報の確認も、上述の復号アルゴリズム等についての署名情報の確認と同様な方法で行えばよい。同様に、特定のマスター鍵の削除指示を外部ネットワークから受け付けた場合にも、署名情報を確認してそれが正当である場合にのみ特定のマスター鍵を削除することとしてもよい。

（１０）本実施の形態では、メモリカードの認証を行い（ステップＳ４０１）、認証に失敗した場合には暗号化及び記録を行わないこととしたが（ステップＳ４０２等）、認証に失敗した場合に最終的にメモリカードへの記録がなされなければよいのであって、例えば、認証に

失敗するか否かにかかわらず暗号化は行い、認証に失敗したならば暗号化の結果生じるデータのＣ２コンテンツ処理部１２１０からの出力を抑止するようにしてもよい。

（１１）本実施の形態で示したメモリカードへ暗号化したデータを記録するため手順は（ステップＳ４０６、Ｓ４０８、Ｓ４０９）、この順に限定されることはなく、いかなる順序で実行されるものであってもよい。また、同じメモリカードに複数のコンテンツのデータを記録することもでき、この場合、タイトル鍵生成部１２２１は、コンテンツの数だけタイトル鍵を生成し、タイトル鍵暗号化部１２２２も前記コンテンツの数だけの暗号化されたタイトル鍵を出力し、オーディオデータ暗号化部１２２３も前記コンテンツの数だけの暗号化されたデータを出力する。

（１２）本実施の形態では、著作権保護センタによりカプセルが生成されることとしたが、これに限定されることはなく、コンテンツ提供者やプロバイダ等が生成することとしてもよい。また、この場合に鍵データの安全性を高めるため、コンテンツ提供者やプロバイダ等が公開鍵を使ってカプセル固有鍵を暗号化し、再生装置側が、当該公開鍵に対応する秘密鍵を用いて復号することとしてもよい。

（１３）本実施の形態では、課金処理として、送金の指示情報等が送信されることとしたが、これに限定されることはなく、課金情報に復号した回数等を含ませ、この課金情報を課金機関向けに暗号化して送信することとしてもよい。また、この際、課金情報をコンテンツとみなし、カプセルと同一のフォーマットで暗号化して送信することとしてもよい。このためには、Ｃ１コンテンツ処理部１１４０及びＣ２コンテンツ処理部１２１０にカプセルを生成するための暗号化部を設ければよい。当該暗号化部における暗号化は、図４、図５に示したカプセル生成の手順に従って行うものとすればよい。

【００５０】なお、記録部１２４０が、メモリカード等の記録媒体にコンテンツを記録する際に、管理情報に含まれる復号条件情報や課金情報をも記録することとしてもよい。この場合にも、復号条件情報や課金情報は暗号化等により安全な状態で記録することとしてもよい。これにより、記録媒体に記録後もコンテンツの再生の実行を制御したり再生実行に対して課金したりすることを可能にできる。

【００５１】

【発明の効果】以上の説明から明らかなように、本発明に係る著作物保護システムは、外部から入力されたデジタル著作物である暗号化されたコンテンツを復号し、記録用に再暗号化して出力する著作物保護システムであって、入力されたコンテンツを第１の暗号方式で復号する復号手段と、前記復号手段により復号されたコンテンツの全部又は一部を第２の暗号方式で暗号化して出力する暗号化手段とを備え、前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータの通信路が単一の耐タンパ性のあるパッケージに封入され、外部との入出力のための端子が前記パッケージの外部に表出しており、前記復号手段は、前記端子を通じて入力を受け付け、前記暗号化手段は、前記端子を通じて出力することを特徴とする。

【００５２】これにより、暗号化されたコンテンツを一度復号して再度暗号化する過程において、復号されたコンテンツが不正に覗き見されないようになる。また、前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータ通信路は、１チップの半導体集積回路から構成されていることとすることもできる。

【００５３】これにより、復号から再暗号化までの過程が１つのチップ内でなされるため、復号された無防備なコンテンツが電気的、物理的に覗き見することができなくなる。また、前記復号手段あるいは前記暗号化手段は、鍵データを記憶しており、復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムを、前記端子を通じて外部ネットワークよりダウンロードし、前記コンテンツを前記鍵データを用いて前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記鍵データを用いて前記暗号アルゴリズムにより暗号化することとすることもできる。

【００５４】これにより、コンテンツについての暗号化アルゴリズムを随時変更し得るので、暗号の安全性が向上する。また、前記復号手段はさらに、前記端子を通じてコンテンツの復号に関する暗号化された制御情報を取得すると共に取得した制御情報を復号する制御情報復号部と、前記復号部により復号された制御情報に基づいて前記コンテンツの復号を行うコンテンツ復号部とを有することとすることもできる。

【００５５】これにより、コンテンツの復号に関する制御情報、例えば復号条件や課金情報等が、暗号化されているため、コンテンツの復号に関する制御情報の覗き見や改ざんを防止できる。また、前記暗号化手段は、マスター鍵を記憶するマスター鍵記憶部と、ディスク鍵を生成するディスク鍵生成部と、前記マスター鍵を用いて、前記ディスク鍵生成部により生成された前記ディスク鍵を暗号化するディスク鍵暗号化部と、タイトル鍵を生成するタイトル鍵生成部と、前記ディスク鍵を用いて、前記タイトル鍵生成部により生成された前記タイトル鍵を暗号化するタイトル鍵暗号化部と、前記タイトル鍵を用いて、前記復号手段により復号されたコンテンツの一部又は全部のデータを暗号化するデータ暗号化部と、前記ディスク鍵暗号化部により暗号化されたディスク鍵と、前記タイトル鍵暗号化部により暗号化されたタイトル鍵と、前記データ暗号化部により暗号化されたデータとを前記端子を通じて出力する出力部とを有することとすることもできる。

【００５６】これにより、ディスク鍵、タイトル鍵、データと３層化して暗号化し、マスター鍵を有する装置によらなければデータの復号ができないので記録媒体に記録されたデータの安全性は高まり、一般ユーザによる不正コピーが防止できる。また、ディスク鍵及びタイトル鍵を、記録媒体中のユーザがアクセス不可能な領域に書き込むことによりさらに安全性を高められる可能性を持つ。なお、記録媒体がＤＶＤである場合には、ＤＶＤ再生機器に対応できる。

【００５７】また、前記マスター鍵記憶部は、複数のマスター鍵を記憶し、前記ディスク鍵暗号化部は、複数の前記マスター鍵それぞれを用いて、前記ディスク鍵を暗号化することにより、複数の暗号化されたディスク鍵を生成することとすることもできる。これにより、メーカ毎に異なるマスター鍵を用いることとすれば、複数のメーカの記録媒体再生装置により、記録媒体に暗号化された記録されたデータの復号が可能となる。また、単一のマスター鍵ではなく複数のマスター鍵を用いるため、記録媒体再生装置への攻撃に対する安全性が高まる。

【００５８】また、前記暗号化手段はさらに、前記マスター鍵を外部ネットワークよりダウンロードして前記マスター鍵記憶部に追加する、あるいは、特定マスター鍵を無効化するマスター鍵制御部を有することとすることもできる。これにより、マスター鍵を追加することができるため、新たな記録媒体再生装置が生産された場合にも対応できる。

【００５９】また、前記暗号化手段により暗号化の結果として得るデータは、記録媒体に記録されるべきものであり、前記記録媒体には、予め媒体に固有な固有情報が記録されており、前記ディスク鍵生成部は、前記記録媒体中の前記固有情報に基づいて前記ディスク鍵を生成することとすることもできる。

【００６０】これにより、記録媒体毎に異なる暗号化が行えるので暗号の安全性が高まり、また、記録媒体からデータを再生する装置側において、ディスク鍵と、記録媒体中の固有情報とを参照することにより記録が正当に行われたものか否かを調べることができ、正当なものである場合にのみ再生を行うようにすることもできる。また、前記タイトル鍵生成部は、前記復号手段により復号されたコンテンツの一部の情報、又は前記暗号化手段に固有な情報に基づき、前記タイトル鍵を生成することとすることもできる。

【００６１】これにより、コンテンツ毎に異なる暗号化が行えるので暗号の安全性が高まり、また、不正コピーがなされた場合に不正な機器の特定に役立つことが期待できる。また、前記記録媒体は、記録装置認証部を備え、前記出力部は、前記記録媒体の前記記録装置認証部から受信する認証情報に基づいて前記記録媒体の正当性を判定し、正当である場合にのみ、前記出力を行うこととすることもできる。

【００６２】これにより、内容の覗き見が容易な不正な記録媒体への記録を防止することができる。また、前記復号手段は、前記コンテンツの復号に際し、当該復号に対する課金処理を行うこととすることもできる。これにより、コンテンツの復号に対して料金を課することが可能となり、コンテンツの販売が容易となる。

【００６３】また、前記復号手段あるいは前記暗号化手段は、外部ネットワークよりダウンロードした復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムについて署名情報を確認して、正当であった場合にのみ、以後、前記コンテンツを前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記暗号アルゴリズムにより暗号化することとすることもできる。

【００６４】これにより、出所の正当な復号アルゴリズムあるいは正当な暗号アルゴリズムのみを取得することができるので、不正なアルゴリズムの置換を防止できる。また、前記マスター鍵制御部は、外部ネットワークよりダウンロードした前記マスター鍵について署名情報を確認して、正当であった場合にのみ、前記マスター鍵を前記マスター鍵記憶部に格納する、あるいは、無効化制御について、著名情報を確認して、正当であった場合にのみ、前記特定マスター鍵の無効化を行うこととすることもできる。

【００６５】これにより、出所の正当なマスター鍵のみを取得することができるので、不正利用を防止できる。また、前記パッケージは、記録媒体に前記コンテンツを記録する記録装置に内蔵され、前記暗号化手段は、前記記録媒体に前記コンテンツの全部又は一部を記録するための所定の規格化された暗号化方式に従った暗号化を行うものであり、前記復号手段に入力される前記コンテンツに施されている暗号化は、前記コンテンツの配送元と、前記記録装置との間における特有の暗号化方式により、前記コンテンツを安全に配送するためになされたものであることとすることもできる。

【００６６】これにより、記録媒体への記録装置に対しての配送のために暗号化されて送られるコンテンツを、記録媒体への記録用の規格化された暗号化に変えて記録することができ、この暗号の変換の過程で生ずる生のコンテンツを覗き見されることがないので、記録装置への配送から記録媒体の記録までの一連の過程における安全性が確保される。

【図面の簡単な説明】

【図１】本発明に係る著作物保護システムの実施の形態である音楽コンテンツ再生記録システム１０００の外観図である。

【図２】音楽コンテンツ再生記録システム１０００の機能ブロック図である。

【図３】メモリカードライタ１２００のハードウェア構造を示す図である。

【図４】暗号化Ｃ１コンテンツ１３０及び暗号化Ｃ２コンテンツ１４０の生成過程を示すデータフロー図である。

【図５】暗号化カプセル固有鍵１１０及び暗号化管理情報１２０の生成過程を示すデータフロー図である。

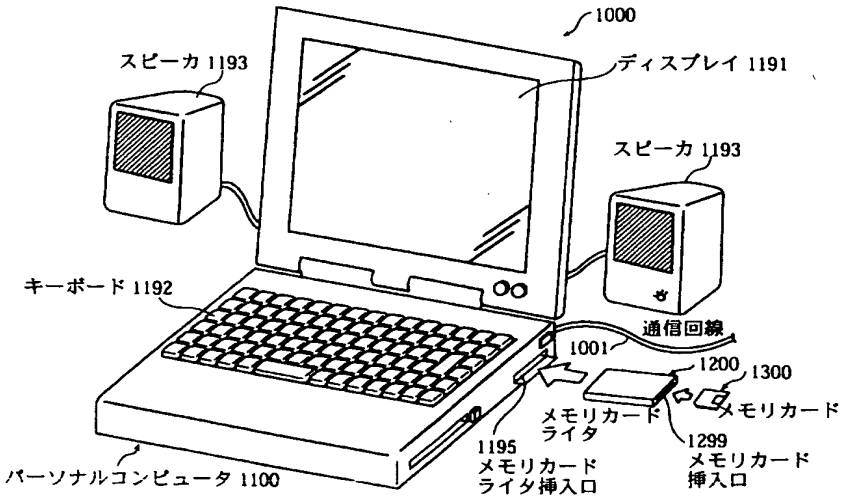
【図６】音楽コンテンツ再生記録システム１０００の動作を示すフローチャートである。

【図７】メモリカードへのオーディオデータの記録のための暗号化と記録処理を示すフローチャートである。

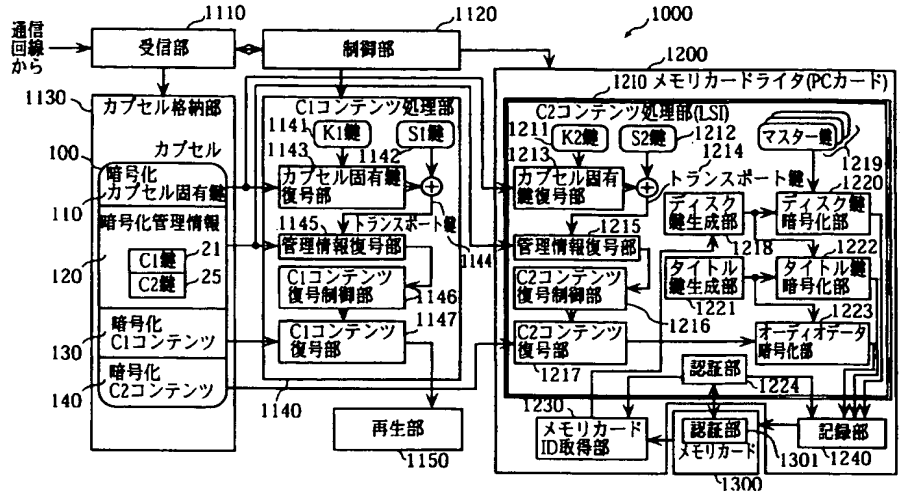
【符号の説明】

１０００	音楽コンテンツ再生記録システム
１００１	通信回線
１１００	パーソナルコンピュータ
１１１０	受信部
１１２０	制御部
１１３０	カプセル格納部
１１４０	Ｃ１コンテンツ処理部
１１４３	カプセル固有鍵復号部
１１４５	管理情報復号部
１１４６	Ｃ１コンテンツ復号制御部
１１４７	Ｃ１コンテンツ復号部
１１５０	再生部
１１９１	ディスプレイ
１１９２	キーボード
１１９３	スピーカ
１１９５	メモリカードライタ挿入口
１２００	メモリカードライタ
１２０１	ＣＰＵ
１２０２	ＲＯＭ
１２０３	ＲＡＭ
１２０４	ＰＣインタフェース
１２０５	メモリカードインタフェース
１２１０	Ｃ２コンテンツ処理部
１２１３	カプセル固有鍵復号部
１２１５	管理情報復号部
１２１６	Ｃ２コンテンツ復号制御部
１２１７	Ｃ２コンテンツ復号部
１２１８	ディスク鍵生成部
１２２０	ディスク鍵暗号化部
１２２１	タイトル鍵生成部
１２２２	タイトル鍵暗号化部
１２２３	オーディオデータ暗号化部
１２２４	認証部
１２３０	メモリカードＩＤ取得部
１２４０	記録部
１２９９	メモリカード挿入口
１３００	メモリカード
１３０１	認証部

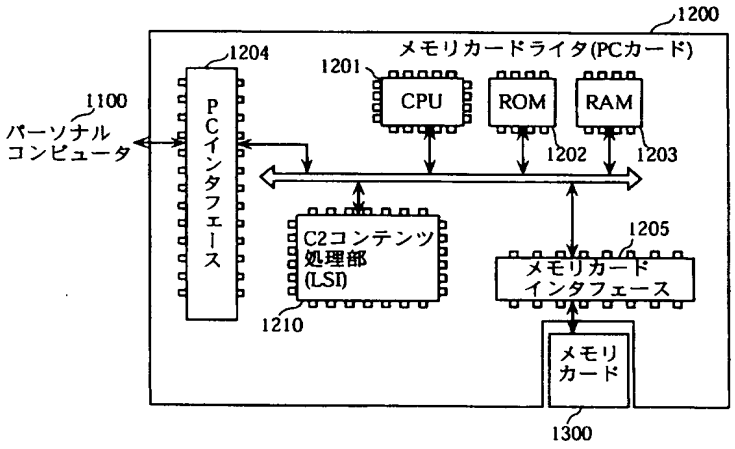
【図１】



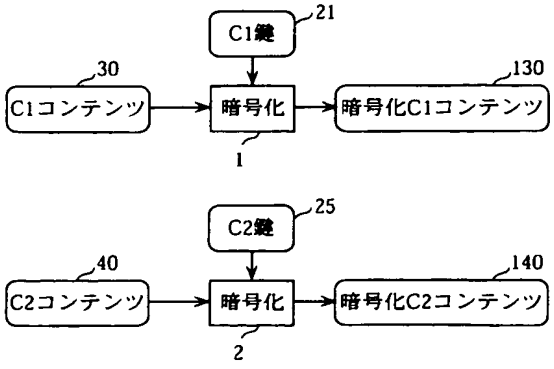
【図２】


通信回線から
受信部
制御部
1000
1200
1210 メモリカードライタ(PCカード)
1110
1120
1130
カプセル格納部
カプセル
100
暗号化カプセル固有鍵
110
暗号化管理情報
120
C1鍵
21
C2鍵
25
暗号化C1コンテンツ
130
暗号化C2コンテンツ
140
C1コンテンツ処理部
1141
K1鍵
S1鍵
1143
1142
カプセル固有鍵復号部
1145
トランスポート鍵
管理情報復号部
1144
C1コンテンツ復号制御部
1146
C1コンテンツ復号部
1147
1140
再生部
1150
C2コンテンツ処理部(LSI)
1211
K2鍵
S2鍵
1212
マスター鍵
1213
1214
1219
カプセル固有鍵復号部
トランスポート鍵
1220
ディスク鍵生成部
ディスク鍵暗号化部
1215
管理情報復号部
1218
1222
タイトル鍵生成部
タイトル鍵暗号化部
C2コンテンツ復号制御部
1221
1216
1223
C2コンテンツ復号部
オーディオデータ暗号化部
1217
認証部
1224
1230
メモリカードID取得部
認証部
メモリカード
1301
記録部
1240
1300

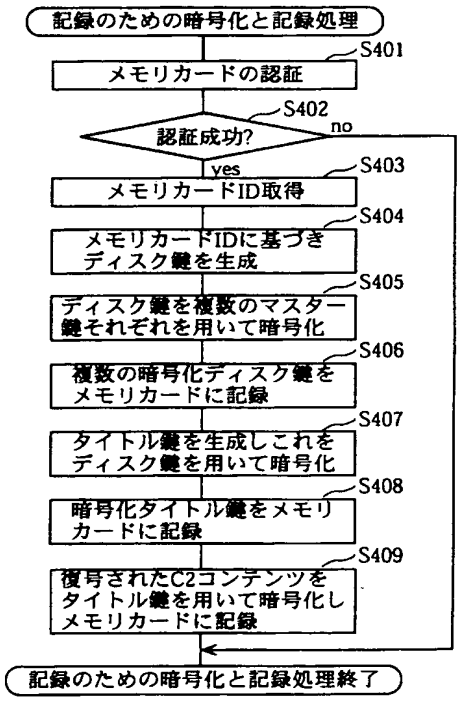
【図３】


1200
メモリカードライタ(PCカード)
1204
1201
CPU
ROM
RAM
1100
パーソナルコンピュータ
PCインタフェース
1202
1203
C2コンテンツ処理部(LSI)
1205
メモリカードインタフェース
1210
メモリカード
1300

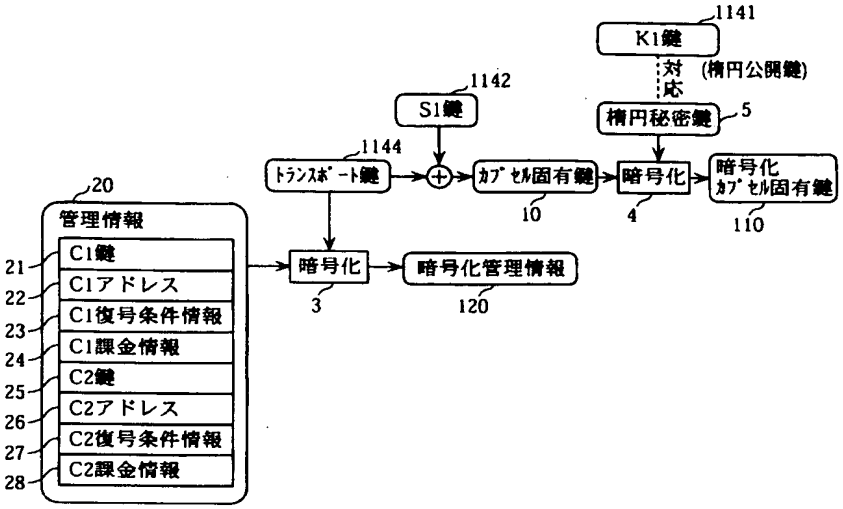
【図４】


C1鍵
21
30
C1コンテンツ
暗号化
130
暗号化C1コンテンツ
1
C2鍵
25
40
C2コンテンツ
暗号化
140
暗号化C2コンテンツ
2

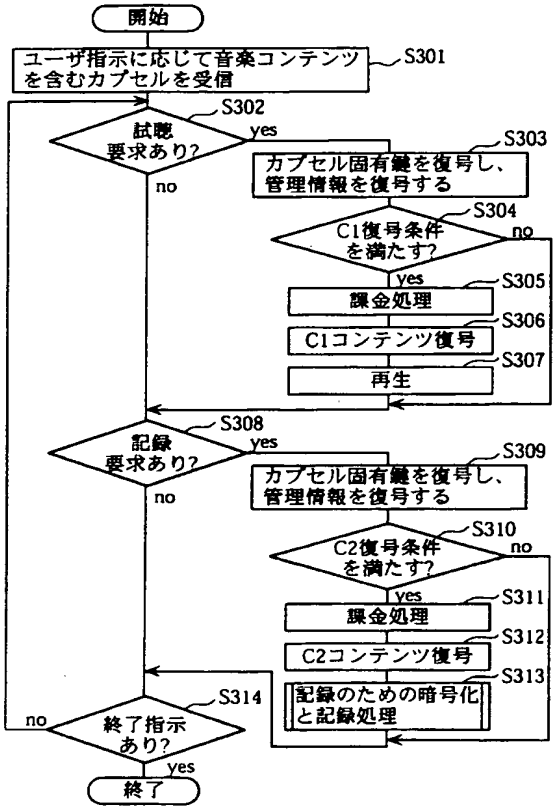
【図７】


記録のための暗号化と記録処理
S401
メモリカードの認証
S402
認証成功?
no
yes
S403
メモリカードID取得
S404
メモリカードIDに基づきディスク鍵を生成
S405
ディスク鍵を複数のマスター鍵それぞれを用いて暗号化
S406
複数の暗号化ディスク鍵をメモリカードに記録
S407
タイトル鍵を生成しこれをディスク鍵を用いて暗号化
S408
暗号化タイトル鍵をメモリカードに記録
S409
復号されたC2コンテンツをタイトル鍵を用いて暗号化しメモリカードに記録
記録のための暗号化と記録処理終了

【図５】


1141
K1鍵
対応
(楕円公開鍵)
1142
S1鍵
楕円秘密鍵
5
1144
ﾄﾗﾝｽﾎﾟｰﾄ鍵
ｶﾌﾟｾﾙ固有鍵
暗号化
暗号化
ｶﾌﾟｾﾙ固有鍵
10
4
110
20
管理情報
C1鍵
C1アドレス
C1復号条件情報
C1課金情報
C2鍵
C2アドレス
C2復号条件情報
C2課金情報
21
22
23
24
25
26
27
28
暗号化
暗号化管理情報
3
120

【図６】


開始
ユーザ指示に応じて音楽コンテンツを含むカプセルを受信
S301
S302
試聴要求あり?
yes
no
S303
カプセル固有鍵を復号し、管理情報を復号する
S304
C1復号条件を満たす?
no
yes
S305
課金処理
S306
C1コンテンツ復号
S307
再生
S308
記録要求あり?
yes
no
S309
カプセル固有鍵を復号し、管理情報を復号する
S310
C2復号条件を満たす?
no
yes
S311
課金処理
S312
C2コンテンツ復号
S313
記録のための暗号化と記録処理
S314
終了指示あり?
no
yes
終了

フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		テーマコード(参考)
Ｈ０４Ｌ 9/10		Ｈ０４Ｌ 9/00	６２１Ａ	

Ｆターム(参考) 5B017 AA06 BA05 BA07 BB03 BB07
CA11 CA14 CA16
5D044 AB05 CC04 GK17 HL01 HL11
5J104 AA07 AA46 JA21 KA02 KA05
NA05 NA36 PA05 PA07 PA10